

## REMARKS

Claims 1-3 are pending. Claims 1-3 stand rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 32 of U.S. Patent No. 6,662,166. Claims 1-3 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,546,471 to Merjanian.

Reconsideration is requested. No new matter is added. Claims 2-3 are amended. The rejections are traversed. Claims 1-3 remain in the case for consideration.

## REJECTION OF CLAIMS AS DOUBLE PATENTED

A terminal disclaimer is filed herewith to overcome the double patenting rejection.

## REJECTION OF CLAIMS UNDER 35 U.S.C. § 102(e)

Merjanian teaches an ergonomic fingerprint reader apparatus. The apparatus is designed in such a way as to support easy and comfortable reading of a fingerprint. Merjanian goes on to provide some example applications (columns 9-12), but the focus of Merjanian is on the device itself, not its uses.

The Examiner appears to have confused the term "identification" as used in the claims, with the terms "authorization" and "verification" as used in Merjanian. This confusion is a fundamental problem with the application of Merjanian as prior art to the invention. To help illustrate the difference between the terms, the Examiner is invited to consider the plain meaning of the terms. "Identification" refers to the process of identifying someone: that is, "identification" answers the question of "Who am I?". Note that this question is open-ended, and the answer is the person's identity.

In contrast, "verification" and "authorization" refer to the process of confirming that a previously-provided identity is correct. In other words, these processes answer the question of "Am I who I say I am?". A common example of verification and/or authorization is the use of personal identification numbers (PINs) used at ATMs. It should be readily apparent that anyone could slide the ATM card into the machine. To help verify that the person using the card is the person authorized to use the card, the person has to enter the PIN that corresponds to the card. If the provided PIN matches that associated with the card, then the user is presumed to be the proper user; if not, then the transactions are refused.

This difference is important, because verification and authorization are two-step processes; identification is a one-step process. In verification and authorization systems (such as Merjanian), the user must first somehow identify himself to the system. This is

typically accomplished by providing something known to be unique to a single person (although not necessarily usable only by that person): for example, a credit card. A credit card has an account number that identifies a single person. This makes verification and authorization very easy: the biometric needs to be compared with only the biometric associated with that credit card number. If the provided biometric matches the biometric associated with the account, then the user is verified or authorized; if it does not match, then the user is not verified or authorized.

Although the above discussion centers on credit cards, a person skilled in the art will immediately recognize that any uniquely identifying information can be used to identify the individual. Most people have many different identifying data; they simply do not recognize it. For example, social security card numbers, bank account numbers, and numbers assigned by other registrars (e.g., universities or doctor's offices) all uniquely identify people, to name but a few examples.

The Examiner might respond that certain numbers, such as a credit card account number, do not uniquely identify a person. For example, typically a husband and wife share the same credit card account number. The Applicant acknowledges this fact. But this does not change the fact that Merjanian teaches a verification or authorization system. Even if multiple people are associated with a particular identifying data, the system is still only attempting to verify or authorize the individual: the system still responds with either a "yes" or "no" message, depending on whether the provided biometric matches a biometric associated with the single account. This shows that Merjanian is not teaching a system to identify individuals: the system cannot say which user associated with the account provided the biometric; the system can only indicate that some user, whose biometric is associated with that one account, is accessing the account.

It should now be clear that prior art systems, like Merjanian, are two-step processes: they depend on the user to first identify himself or herself before he or she can be verified/authorized. Merjanian glosses over this fact, but this first step is implicitly discussed. For example, at column 10, lines 34-36, Merjanian says that "the person presenting the card or stamps is compared with a store of authorized operators". In other words, before the comparison can be made, the authorized operators must be identified. This theme is constant in Merjanian: each example requires the user to first identify himself or herself, before the comparison can be made.

In contrast, the claimed invention requires no pre-identification step. Note, for example, that claim 1 describes "the electronic identifier compar[ing] the payor's bid

biometric sample with at least one registered biometric sample”: no limit is put on which registered biometric samples the bid biometric sample is compared with. Claim 1 goes even further: it describes the result of this comparison as being “for accessing the payor’s previously registered account data”. In other words, the account data is not known until after the comparison is complete. Merjanian clearly teaches away from the claimed invention, in that Merjanian requires that the account data be known before the comparison is made. Claims 2-3 are similar to claim 1, in that the purpose of comparison is to identify the account data: that is, to identify the individual.

The Examiner might argue that the personal identification code discussed in claims 2-3 identifies the user. This would be incorrect. As described at page 8, lines 8-16, the personal identification code (a PIN) is selected by the user. This implies two facts. First, if the user is selecting the PIN, then the PIN is not being assigned to him by the system. This means that the system cannot guarantee that the user’s PIN is unique to the user. Second, it is highly unlikely that the user will select a unique PIN; people by their very nature do not pick PINs long enough to be unique. For example, there are roughly 300,000,000 people in the United States. Even if we could assume that everyone would magically pick unique PINs, that would require a PIN of at least nine digits. But most PINs are between four (the original standard established by banks) and six digits long (dates are typically six digits long, and so are easy to memorize). Clearly, PINs that are not long enough to uniquely identify people cannot be expected to be unique, and so cannot be used to identify the individual.

The rationale for the PIN in the claimed invention is to reduce the search space of biometric samples. The PIN provides a clue as to which set of biometrics might include the user. But the system is still identifying the user from that set. That the system returns the account data of the user shows that the system is performing identification, and not verification/authorization.

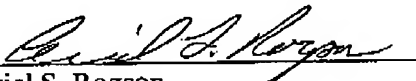
The Examiner’s discussion about Merjanian teaching set-top box notarization suffers from the same problems as those discussed above. Notarization does not identify a particular user: it certainly does not identify the account data from all accounts stored in the system. It is worth noting that the Merjanian explicitly teaches that “[c]redit card data, which may include the account number, type of card, expiration date, name of owner, etc., is conveyed along with compressed fingerprint data to serve as the operator’s notarization that the transaction has been authorized against the identified credit, debit, or smart card account” (column 12, lines 28-33). In other words, the fingerprint data is not identifying the account; if it were, the credit card data would not be needed.

Finally, it is worth noting that the examples given by Merjanian are all token-based. For example, in column 12, line 23 describes the receiving device as storing "credit, debit, or smart card account information". In other words, the account being used is represented on such a card. But these cards are "tokens"; the claims make clear that the system and method are "tokenless": that is, without such cards.

For the reasons presented above, claims 1-3 are patentable under 35 U.S.C. § 102(e) over Merjanian. Accordingly, claims 1-3 are allowable.

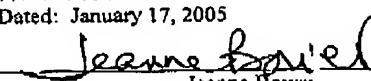
For the foregoing reasons, reconsideration and allowance of claims 1-3 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,  
MARGER JOHNSON & McCOLLOM, P.C.

  
Ariel S. Rogson  
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.  
1030 SW Morrison Street  
Portland, OR 97205  
503-222-3613  
Customer No. 20575

I hereby certify that this correspondence is being transmitted to Mail Stop AMENDMENT, U.S. Patent and Trademark Office, via facsimile number: 703/872-9306.  
Dated: January 17, 2005

  
Jeanne Bower